CHILDREN AND THEIR DIGITAL DOSSIERS: LESSONS IN PRIVACY RIGHTS IN THE DIGITAL AGE

ILENE R. BERSON
MICHAEL J. BERSON

The right to privacy is a firmly entrenched democratic principle that has been inferred in the U.S. Constitution and protected by the Fourteenth Amendment as a liberty of personal autonomy.[1] Although the Constitution does not include language that explicitly details privacy protections, since the 1800s justices have interpreted the text as promoting the "right to be left alone."[2] Evidence of compelling support for protection of privacy also has been found in several of the Constitutional Amendments, including the First, Fourth, Fifth, and Fourteenth.[3]

However, it is the statutory right to privacy that has been most closely aligned with data protection as a form of self-protection. The U.S. Federal Trade Commission has led efforts to enforce compliance with privacy. The statutory right of privacy limits access to personal information and has been extolled in the proliferation of privacy policies and legislation that control the collection of information about children on the Internet.[4]

Despite the longstanding tradition of individuals controlling access to and use of personal information, technology has expanded the flow of identifiable data into the public domain. Students' rights and protections are emerging as a key public concern,[5] and the public documentation and tracking of young lives through Web logs or blogs, e-journals, digital photos, Web pages, online profiles, radio frequency identification, and other forms of data surveillance have complicated efforts to safeguard young people's privacy protections in digital spaces. This article explores controversies over the protection of children's privacy in a digital age and discusses connections between online privacy, cyber-identity, and self-protection in a democratic society.

Children and Privacy in Cyberspace

A full exploration of privacy issues is beyond the scope of this article, and the purpose of this discussion is not to debate restrictions or control for access to public documents. The intent is to explore how young

people interact and manage within an information age where information flows so easily and can be used for numerous ulterior interests.

While digital technologies offer new ways for children and youth to obtain information, the interactive nature of the Internet creates prime opportunities for young people to engage in activities which compromise their privacy or well-being. The captivating world of cyberspace is a "seductive and potentially manipulative environment for children,"[6] and the capacity of young people for self-regulation is often limited. The digital environment creates many opportunities for gathering data from children and sending them targeted messages. Individuals, organizations, and companies have used the World Wide Web to access youth and impinge upon their privacy by eliciting personal information through online registration forms, Web profiles, Internet quizzes/surveys, entry forms, electronic postcards, and coupons/promotional activities. The collection of personal information from the young capitalizes on their deficits in understanding the strategies that are used to engage children online and a lack of awareness of the Internet's unique capacity to mine data and track individual users.

Although information itself may not be a threat, use of the data may pose a danger. The compilation, storage, and sale of public information is a large industry in the United States, and often includes public information from commercial sources as well as government records on individuals. These collections of information are referred to as digital dossiers.[7] Daniel Solove has described the aggregation of information about individuals as an unauthorized digital biography that is often filled with erroneous details and data that have been taken out of context to yield a distorted persona.[8]

The Web is serving as a major information delivery mechanism that is a rich source of information for organizations, companies, and individuals that want to capture the interests, behaviors, and habits of young Web users. Children are a highly marketed segment of the consumer population, and young people often serve as information brokers for their own personal information as well as data about their friends. Students create digital personas, which represent a complex interaction between the data that they encounter and the data that they give out.

Sophisticated technology has evolved extensive information dissemination systems that represent a contemporary intrusion to privacy. Since the First Amendment protects the right to speak and publish information, digital dossiers often are comprised of public-domain documents that may have been freely provided to third parties by an individual. For adolescents, extensive use of online journals and participation in Internet communities can offer another medium in which personal information is disclosed to strangers. Caregivers struggle to balance the child's need for

personal privacy and independence with safety concerns in a digital environment.

In the United States, privacy can be best achieved by controlling nondisclosed information. Once personal data has been released, there is little that can be done to curtail its dissemination or accumulation into enormous databases where digital dossiers evolve from the collective accumulation of information that has been combined, indexed, and correlated. These dossiers can then be used to judge and evaluate individuals, establish a profile, and determine "desirability."[9] These extensive histories can degrade tolerance for negative activities and diminish young people's opportunities to learn life's lessons and receive social forgiveness for indiscretions.

Among the issues that caregivers and child-serving professionals need to understand is the interface between online access and potential infringements to privacy protection. Prior to the Internet, data on an individual existed in many unrelated databases, and this disconnect had a protective function to privacy. The merging of data reveals the vulnerability of confidential information. The Internet's interactive nature creates a forum whereby children can be targeted individually and engaged in efforts to track their identity and/or behavior online. The gaze of cookies and Web bugs that are posted during online sessions facilitate collection, storage, and data matching. Additionally, the collection and retrieval of information in cyberspace creates a context where fallacious or deleterious information can become archived. Human tendencies to be reductionistic in thinking (i.e., the reductionist fallacy) may rely on erroneous information or give excessive prominence to the "worst truths," which may subsequently achieve prominence and create barriers to facilitating behavioral change. As a result, past mistakes or educational problems can become lifelong burdens that drive expectations.

As insidious as the hoarding, abuse, and misuse of data may be, a more obscured phenomenon may be taking place whereby young people are increasingly desensitized to the loss of control over their personal information. There appear to be varying views on the ability of children and youth to effectively manage information and make informed decisions about the implications of willingly providing personal information to others. For parents and educators, it is a challenge to persuade children and youth to safeguard their personal data. Several studies have demonstrated that young people freely reveal private information.[10] Developmentally, children typically do not begin attenuating to risk until middle childhood, thereby necessitating that adults serve critical protective roles. Even in the teen years, the ability to make informed life choices is still in a state of flux.[11] Adolescents have often been described as particularly vulnerable to risky behavior, including poor decision-making.[12]

Technotracking of Children: When Child Protection and Personal Privacy Collide

Increased sensitivity about infringements to privacy combined with recent events, including school shootings, child abductions, and terrorist acts, have intensified concerns over potential threats to children's safety and security. This concern has manifested itself in numerous technological developments that have been designed or adapted to protect children and prevent harm. However, technology has an adverse side, and its role in surveillance has raised concerns about privacy. Debate is ensuing over whether technology is the right solution for child protection concerns.

Modern technology has provided the means to track children. Opponents of technotracking believe that a reliance on technology introduces infringements to privacy that are too great a price to pay for better security.[13] However, communities around the world are exploring various options with mixed results.

As the price of technology solutions continues to drop, parents are increasingly enticed by many emerging products that focus on monitoring the whereabouts of children, and schools are seeking out new ways to ensure the safety of the children in their care. One example involves radio frequency identification technology, or RFID. Using a technology that has been used by retailers to track merchandise and by ranchers to monitor livestock, embedded computer chips are each programmed with a unique number, and a tiny antenna transmits the information to nearby scanners. Some school authorities in Japan and the United States have introduced student identification tags on name badges, clothing, or backpacks.[14] The RFID chips are scanned and track students when they enter the school building. A company in Mexico has taken this one step further by offering a service to implant microchips in children as an anti-kidnapping device.[15]

Malls and amusement parks in the United States and Denmark have also looked to technology to help parents keep track of their children.[16] Using a combination of RFID and wireless technology, wristbands can be rented that broadcast a signal, and the location of a child can be retrieved from kiosks. The devices also have other features and can be used to send messages among members of the family or to locate nearby restaurants or restrooms. A similar device using GPS technology is marketed by a company, allowing parents to access information about their child's whereabouts through a simple phone call. Whereas the RFID devices have a short-range capacity and are most ideal for confined spaces, the GPS devices pinpoint the location of children in real time and can replay their whereabouts over the last few hours. Some also feature panic buttons that can instantly alert a parent via phone in case of an emergency.

While some features of the technology are perceived to be beneficial, the implementation of this technology has initiated debates over the trade-offs between security and privacy. In the United States, various groups like the American Civil Liberties Union and the Electronic Frontier Foundation argue that technosurveillance of children breaches rights to privacy and treats children like inventory.[17] Concerns have been expressed that the safety and security of students could be jeopardized. Although children in most countries do not have the same rights to privacy as adults, opponents assert that the limited rights of children are unfairly negated by this technology. There have been outcries in Europe that children's privacy might be infringed upon by identity cards that carry health information about a child.[18] In the United States parents typically have authority over children's information, and the Supreme Court has "recognized three reasons justifying the conclusion that the constitutional rights of children cannot be equated with those of adults: the peculiar vulnerability of children; their inability to make critical decisions in an informed, mature manner; and the importance of the parental role in child rearing."[19] There are no clear rules in the United States prohibiting parents from using technosurveillance in their families. Therefore, American parents generally have tremendous latitude in monitoring the whereabouts of their children. In contrast, U.S. laws have been passed to safeguard children from privacy invasions by others. For example, the Children's Online Privacy Protection Act of 1998 restricts Web site operators from collecting and disseminating information pertaining to patrons under the age of thirteen.[20]

Individual families will continue to grapple with privacy issues and the appropriateness of technotracking as well as the impact on the parent-child relationship; however, the infusion of this technology into public spaces, such as schools or malls, creates widespread concerns about the transformation of a device to protect safety to one that could be abused by others. Questions such as what happens to the data collected and who has access to the tracking information are especially salient in light of recent events in which data has been breached by unauthorized users or for unintended purposes. In Northern California, the use of RFID devices in a school district was abandoned after parents and privacy advocates objected to tracking children without caregiver knowledge or consent.[21]

Opponents also have warned that techsavvy kids will eventually figure out how to manipulate the devices into falsely reporting their location. Since the devices can be easily removed from the body of a child, either the child or others may be motivated to fool the device. Additionally, technotracking services could be used as a tool of stalkers, kidnappers, child predators, etc. to pinpoint the location of children in

real time.

Although companies producing the devices have countered that privacy protections have been designed in the system, such as limited range of ID readers and active scanning by touching a screen rather than passive detection of identification tags, evolving capabilities and adaptations of the technology could result in incidents in which the identity and location of a child is broadcast to anyone with a chip reader. The remote readability of the chips and lack of encryption have raised concerns that this security solution does not adequately mitigate the risks, and instead it creates additional risks due to the data collected. Technical insecurity of the systems combined with potential inaccuracies that generate misleading information about a child's location suggests that this form of surveillance currently lacks sufficient security to safeguard vulnerable children.[22]

Child Protection in a Digital Environment

The duty of adults to assume a proactive role is necessitated by the vulnerability of children and youth to malicious behavior, including those who would take advantage of the insecurities and naiveté of youth to maximize their access to personal information. Although caregivers and child-serving professionals may play an essential role, they tend to have only limited understanding of technology and appropriate prevention initiatives for children. American adults "have no clue about data flows—the invisible, cutting edge techniques whereby online organizations extract, manipulate, append, profile and share information about people on-line."[23] Consequently, as society struggles to address the serious social problems associated with Internet use, adults often find themselves inadequately prepared to assist children in understanding the complexities of privacy issues in a digital age.

Recognizing the vulnerability of children to privacy infringements, the United States has passed legislation that requires commercial Web site operators to acquire parental consent before personal information is collected from children under age thirteen. The law, known as the Children's Online Privacy Protection Act (COPPA),[24] is enforced by the Federal Trade Commission. COPPA denotes that Web sites that are directed to children under thirteen are prohibited by law from making a child's participation conditional on the provision of personal information. Nonetheless, although safeguards must be in place regarding the collection of personal information from children, COPPA does not preclude the acquisition of information or linking information with other data on the child that has been collected digitally. Parents can maintain control by accessing, changing, or deleting their child's personal information.

COPPA also stipulates that teachers can act on behalf of parents in

the school setting so that students can engage in online activities that the teacher feels have an educational benefit. School districts also must have policies to protect student privacy as a provision stipulated under the Elementary and Secondary Education Act of 2001.[25] Schools need to safeguard against violation of students' privacy through posting of names and photos on school Web sites; the disclosure of confidential student information via staff emails and other electronic communication; and the distribution of private information by other students.

Although COPPA relies on caregivers and teachers to defend children's safety and privacy online, the proliferation of technology has been accompanied by a rise in the public documentation of children's lives through blogs and public journals. Parental publishing of children's life experiences from birth is increasingly common, and the task of documenting lives online is often usurped by children at young ages as they learn to interact in digital spaces. By the time children in the United States turn thirteen years old, they are viewed by the statutes as legally capable to make their own decisions when communicating electronically.[26] Adults responsible for children, whether caregivers or other child-serving professionals, need to engage in careful deliberation before placing young people's personal information on the Internet or using technology to track student data and records, since it establishes an early precedent for subsequent online choices made by young people.

Although the details of minors are protected by COPPA, young people, who are increasingly exposed to a proliferation of personal information on the Internet, are becoming desensitized to the digitization of public records. Subsequently, youth often remain oblivious to ways to maximize the privacy of their online activities. They remain naive regarding social dangers and accessibility of online communications, even as access to electronic records becomes increasingly ubiquitous via handheld PDAs, mobile phones, and other devices.

Digital Literacy for Effective Citizenship

The pervasiveness of technology in homes and schools has afforded the benefit of access to resources while simultaneously evolving the emergence of social problems in the digital space. The diffusion of the Internet into the lives of children can expose them to information with questionable legitimacy, ideas that can be contrary to positive behaviors, and messages that are intended to manipulate their actions or beliefs.[27] Additionally, new issues have arisen as information technology gains prominence in the national infrastructure, accelerating the capacity for economic opportunities and opening communication. Society is increasingly recognizing that these technology-based assets must be protected from threats to security.

Due to the omnipresence of technology, young people require critical-reasoning skills to facilitate their active engagement with information. Digital literacy builds the foundation for productive functioning as a global citizen and addresses the development of skills needed for the evolving cyber-domain.

Digital literacy is a compilation of legal precedent, voluntary policies, and ethical conduct. It represents the ability to access digital forms of information, critically evaluate its quality and utility, analyze information for connections to and expansions of knowledge, and use digital tools to produce original works. It emphasizes the capacity to fully participate as a responsible member of a technologically engaged society and refers to the skills that people need to understand and constructively navigate the digital media that surrounds them. It addresses safety and security while fostering broader preparation for digitized and networked environments.

Digital technologies are increasingly ubiquitous, and mobile technology adds new layers of vulnerability and accessibility. Pervasive computing can infringe upon privacy protections. Moreover, digital content can be manipulated; therefore, it should be critically evaluated to determine its trustworthiness. Many young people are immersed in an interconnected environment comprised of an enticing amalgamation of images, words, and sounds. While young people have often mastered the task of using the technology tools to communicate, they have typically not acquired the proficiency to function responsibly as members of networked communities. In order to optimize the benefits of a digital society, children and youth need adequate preparation.

Digitally literate individuals appreciate the difference between information and knowledge, and they focus on bridging the gap between the capacity to access data and the skill to synthesize, evaluate, and interpret information for educational benefit. Youth, in today's world, are not only consuming digitized information, they also are actively manipulating, adapting, and disseminating information through communication technologies.[28] However, despite their immersion into this global setting and their enthusiasm for online activities, they often are focused on discrete technical tasks that entail seeking out information, communicating with others, and playing games. Conversely, they lack skills to gauge the influence of digital messages on their behavior or assess the relative risk and manage the challenges of communicating with digital technologies.

The liberating anonymity of the Internet, where children and youth can access and contribute to a vast repository of information, is tempered by methods to track users and aggregate data for use by marketers, Internet regulators, and predators. Therefore, children need instruction on the application of skills for critical analysis and ethical decision making. This includes ongoing practice in controlling disclosure of per-

sonal information. To be successful in this task, young people need to learn to process information so that they can make thoughtful decisions. Access to massive amounts of information necessitates competency in gauging the quality and accuracy of information. In turn, students have an obligation to consider the implications of communication that they initiate via information technologies since the network of recipients is so dynamic and expansive. Messages become publicly accessible and have potentially widespread negative implications.

Ultimately, basic education for safe and responsible choices in digital environments will be increasingly important not only for personal safety, but also to ensure the security of the digital infrastructure. Just as most students acquire an understanding of protection rules for their physical well being, the essential skills for securing personal information in digital formats will lay the foundation for safeguarding protected data. Preventative intervention in the schools may enhance instruction on the extraordinary resources and opportunities available online while simultaneously creating a medium for applied practice in restricting unauthorized digital traffic, discriminating between credible information and messages intended to manipulate thought or action, identifying sources of data, and recognizing that this context is a communication modality for a global community comprised of diverse perspectives and people.

A compelling role for teachers emerges from an awareness of our vulnerabilities due to our new reliance on technology. The obligation of schools is to not only emphasize the mechanics of the use of communication technologies, but also address the social consequences of participating in digital forums. Young people enjoy the power of sharing ideas and communicating with others, and cyberspace offers a globally-connected community in which students are challenged to apply their social competence and ethical decision-making skills within a worldwide forum. To this end, we are obligated to educate children on critical protection and security in a digital age as well as prepare them for cybercitizenship with guidelines for acceptable online behavior.[29]

Thinking and reasoning are at the center of digital literacy. Literacy efforts empower youth to analyze, interpret, and create images and information that are disseminated in digital environments. They provide skills so that youth can decipher complex messages in an informed and knowledgeable way, and they counteract the temptation to react without forethought to the influence of powerful words, images, and sounds. Skills include the critical analysis of digital media, investigation and evaluation of information, consideration of divergent interpretations, recognition of representations of point of view, and the ability to safeguard against vulnerabilities to personal security and safety in cyberspace.

Although youth are well acclimated to the digital medium and have

adjusted rapidly to it, they need specific opportunities to practice skills and develop new habits of respect, empathy, equity, and advocacy in a global context. Digital literacy fosters the knowledge and skills for global citizenship by linking everyday individual actions with the consequences for oneself and others.

Concluding Thoughts

> [W]hen intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences. [30]

> Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge.[31]

Data gathering technologies are becoming increasingly sophisticated and taking many forms. Of greatest concern is how these vast repositories of information are handled in a way that accommodates the values of privacy. As a result, database security has evolved as a critical component of protection and safeguarding of privacy.

Our communities often look to technology as an ideal solution to social problems; however, the real answer may be related to committing and accessing sufficient human resources devoted to child protection. We need to continue to explore both technological and nontechnological approaches to safeguarding children while being cognizant that this is a complex issue that requires careful deliberation of the intended and unintended consequences of tracking children and their data.

Part of the process of safeguarding children's online experiences is the active instruction to educate children to navigate safely in cyberspace. Educational strategies that focus on helping children and youth to develop autonomous and responsible skills online require guided instruction and practice. This approach complements existing filters and security systems that cannot guarantee total protection. Moreover, the introduction of standards-based lesson plans, the creation of developmentally appropriate Acceptable Use Policies, and the inclusion of orientations which address social, ethical, and legal behavior online, can counter infringements against youth and sustain the dynamic and interactive benefits of communication technologies. Despite the alarming incidents that children might experience in cyberspace, preventative intervention may preserve the extraordinary opportunities available online and offer a medium for applied practice in evaluating the credibility of information, understanding sources, and appreciating the diversity of perspectives and people in a global community. Subsequently, youth can help shape social and cultural interaction in a cyberworld that is built on values of respect, responsibility, justice, and tolerance.

Learning to function in a democratic society does not depend on total and complete secrecy. In fact, for children privacy should never be absolute since caregivers are responsible for their protection and need critical information on children's well being and functioning. Moreover, parental monitoring of children and their data promotes engagement of families while insulating children from potential harm. However, for children to achieve autonomy as informed and productive citizens in a digital age, they need opportunities to understand how to regulate personal information as well as make informed judgments to discriminate between benign data versus information that should be protected due to its sensitivity or potential for harm.

As this generation of children grows up immersed in an information age, they may disregard traditional conceptualizations of privacy as a relic of a time when documents were stored in dusty file cabinets in basements. However, whether youth are apathetic to techniques to track them and profile their flow of data into extensive, although sometimes inaccurate, digital dossiers or sensitized to the electronic footprints that they leave behind will depend on instilling in young people the ability to engage in informed cost-benefit analyses of privacy and data flow in an interactive digital society.

Child protection initiatives must therefore not only be concerned with securing the physical environment of the child, but also create opportunities in which children may practice processing information without potential for harm due to indiscretions, explore preferences in an environment that is free of intrusion and embarrassment, and draw conclusions that are independent and immune to manipulation. This integration of privacy and protection agendas may overcome the discontinuity that currently exists for this generation of young people and create a future in which privacy and access to information achieve a homeostatic balance that is simultaneously responsive to the evolving capabilities of new technologies and the democratic principles that foster individual opportunity and autonomy.

NOTES

1. Legal Information Institute, "Right of Privacy: An Overview," http://www.law.cornell.edu/topics/privacy. html.

2. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890): 193-220.

3. Legal Information Institute, *Right of Privacy: An Overview.*

4. For resources on children and privacy see the Federal Trade Commission (FTC), "Kidz Privacy," http://www.ftc.gov/kidzprivacy.

5. For practical tips on how to safeguard personal privacy see Privacy Rights Clearinghouse, www.privacyrights.org.

6. Privacy Rights Clearinghouse, "Fact Sheet 21: Children's Online Privacy,"

http://www.privacyrights.org/fs/fs21-children.htm.

7. For in-depth discussions of digital dossiers, see Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000) and Daniel Solove, *The Digital Person* (New York: New York University Press, 2004).

8. Solove, *The Digital Person.*

9. Rosen, *The Unwanted Gaze.*

10. Ilene R. Berson, Michael J. Berson, and John Ferron, "Emerging Risks of Violence in the Digital Age: Lessons for Educators from an Online Study of Adolescent Girls in the United States," *Journal of School Violence* 1, no. 2 (2002): 51-72; Amanda Lenhart, Mary Madden, and Paul Hitlin, "Teens and Technology: Youth Are Leading the Transition to a Fully Wired and Mobile Nation," *Pew Internet and American Life Project*, http://www.pewinternet.org/PPF/r/162/report_display.asp; Joseph Turow and Lilach Nir, "The Internet and the Family 2000," *Annenberg Public Policy Center*, http://www.annenbergpublicpolicycenter.org/ 04_info_society/info_society.htm.

11. Ilene R. Berson and Michael J. Berson, "Digital Literacy for Cybersafety, Digital Awareness, and Media Literacy," *Social Education* 67, no. 3 (2003): 164-68.

12. Ilene R. Berson, "Making the Connection Between Brain Processing and Cyberawareness: A Developmental Reality," (proceedings of the Netsafe II: Society, Safety and the Internet Symposium, Auckland, New Zealand, September, 30 2003), http://www.netsafe.org.nz/Doc_Library/netsafepapers_ileneberson_cyberaware ness.pdf.

13. Electronic Privacy Information Center, "Children and RFID Systems," http://www.epic.org/privacy/rfid/ children.html.

14. Ibid.

15. Julia Scheeres, *Tracking Junior with a Microchip,* http://www.wired.com/news/technology/0,1282, 60771,00.html.

16. Electronic Privacy Information Center, *Children and RFID Systems.*

17. Electronic Frontier Foundation, *Keep RFIDs Out of Public Schools,* http://www.eff.org/Privacy/Surveillance/RFID/schools; ACLU, *Parents and Civil Liberties Groups Urge Northern California School District to Terminate Use of Tracking Devices,* http://www.aclu.org/StudentsRights/StudentsRights.cfm?ID=17442&c=161.

18. Electronic Privacy Information Center, "Children and RFID Systems."

19. Bellotti v. Baird, 443 U.S. 622 (1979).

20. In 1998 Congress passed the Children's Online Privacy Protection Act (COPPA), which took effect in April of 2000, (15 U.S.C. 6501, or 16 C.F.R §312), www.ftc.gov/ogc/coppa1.htm.

21. Electronic Privacy Information Center, "Children and RFID Systems."

22. Ibid.

23. Joseph Turow, "Americans and Online Privacy: The System is Broken," http://www.appcpenn.org/reports/2003/turow-privacy-no-cover.pdf.

24. COPPA, http://www.ftc.gov/ogc/coppa1.htm.

25. Elementary and Secondary Education Act of 2001, http://www.ed.gov/policy/elsec/leg/esea02/index.html.

26. COPPA, http://www.ftc.gov/ogc/coppa1.htm.

27. Berson, "Making the Connection Between Brain Processing and Cyberawareness"; Berson and Berson, "Digital Literacy for Cybersafety, Digital Awareness, and Media Literacy."

28. Berson, Berson, and Ferron, "Emerging Risks of Violence in the Digital Age."

29. Michael J. Berson and Ilene R. Berson, "Developing Thoughtful 'Cybercitizens'," *Social Studies and the Young Learner* 16, no. 4 (2004): 5-8; Michael J. Berson and Ilene R. Berson, "Lessons Learned about Schools and their Responsibility to Foster Safety Online," *Journal of School Violence* 2, no. 1 (2003): 105-17.

30. Rosen, *The Unwanted Gaze, 9.*

31. Ibid, 8.